The Quest for Visibility and Control in the Cloud

By Yuri Diogenes – ISSA Senior Member, Fort Worth Chapter

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. This article will cover important considerations regarding cloud security visibility and control.

Abstract

Although cloud security has evolved over the years and is becoming more mature, the endless journey to obtain the right level of visibility and control over the cloud workloads is still a challenge. From companies that are still in the process of migrating to the cloud to companies that are already building their infrastructure entirely in the cloud, the governance of cloud workloads can be difficult if not approached correctly and using the right tools. In addition, companies that need to adhere to certain compliance standards must understand the current security controls around their workloads and how they map to the standards that they need to be in compliance with. This article will cover important considerations regarding cloud security visibility and control.

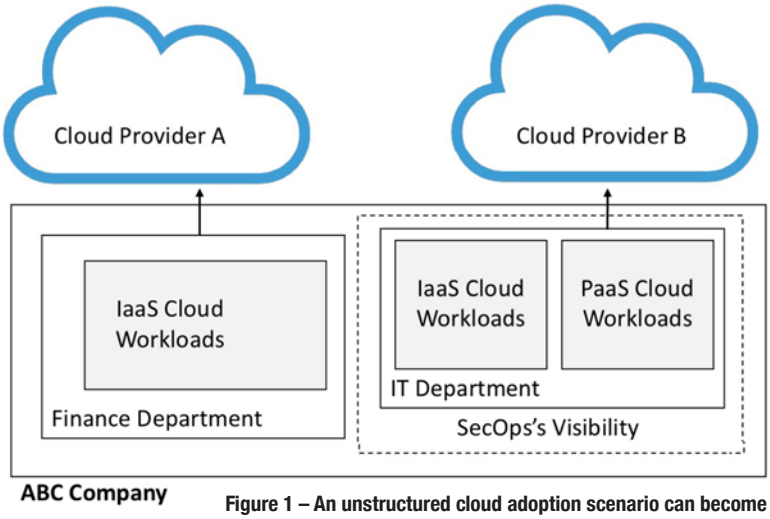

Figure 1 – An unstructured cloud adoption scenario can become a nightmare for the SecOps

According to "The 2018 Global Cloud Data Security Study" conducted by Ponemon Institute,[1] forty-nine percent of the respondents in the United States are "not confident that their organizations have visibility into the use of cloud computing applications, platform, or infrastructure services." According to Palo Alto's "2018 Cloud Security Report,"[2] sixty-two percent of the respondents said that misconfiguration of cloud platforms is the biggest threat to cloud security. What we have here is exactly the lack of visibility and control over different cloud workloads, which not only cause challenges during the adoption, but also slow down migration to the cloud.

In large organizations the problem becomes even more difficult due to the dispersed cloud adoption strategy. This usually occurs because different departments within a company will lead their own way to the cloud, from the billing to infrastructure perspective. By the time security and operations teams become aware of those isolated cloud adoptions, these departments are already using applications in production and integrated with the corporate on-premises network (figure 1).

In addition to this unstructured approach, these adoptions usually are done without proper monitoring planning, and many times the attempt to leverage legacy tools to gain viability to cloud resources does not provide an accurate picture

1 "The 2018 Global Cloud Data Security Study," Gemalto (Jan 2018) – https://safenet.gemalto.com/resource/partnerasset.aspx?id=64424542279&langtype=1033.

2 "2018 Cloud Security Report," Palo Alto Networks (May 2018) – https://www.paloaltonetworks.com/resources/research/2018-cloud-security-report-palo-alto-networks.

ISSA CAREER CENTER

The ISSA Career Center offers a listing of current job openings. Among the current 832 job listings [3/4/19] are the following:

- **Lead Engineer Product & Network Security**, Hill-Rom/Welch Allyn – New York, NY
- **Information Systems Securty Officer (ISSO)**, Modern Technology Solutions, Inc. (MTSI) – Alexandria, VA
- **Cybersecurity Analyst**, IDA – Alexandria, VA
- Business Intelligence Developer, Jackson & Coker – Alpharetta, GA
- **Director - Center of Cyber Security / Tenured Faculty**, College of Science Auburn University at Montgomery – Montgomery, AL
- **Information Security Architect**, Praxair – New York, NY
- **Business Information Security Officer – Military**, General Electric – Evendale, WA
- **Information Security Risk Engineer**, Columbia University – New York, NY
- **Information Security Engineer 5**, Wells Fargo – Charlotte, NC
- **Lecturer - Information Security**, Johns Hopkins University – Baltimore, MD
- **Information Security & Risk Management Manager**, Columbia University – New York, NY,
- **Chief Information Security Officer**, Quinnipiac University – Hamden, CT
- **Information Security Risk Admin**, InTouch Health – Dallas, TX
- **Senior Engineer - Information Security Compliance**, Verisign – Reston, VA
- **AVP, Information Security Risk Assurance Lead Analyst**, Synchrony Financial – Multiple Locations
- **Information Security Analyst – Splunk Developer (L08)**, Synchrony Financial – Hyderabad, IN
- **Instructor, Cybersecurity - BAS (Job #0818)**, Pasco-Hernando State College – New Port Richey, FL
- **Security Engineer,** Washington College – Chestertown, MD
- **Assistant Administrator for IT & Information Security**, GenCanna Global USA, Inc. – Winchester, KY
- **IT Information Security Operations Centre (SOC) Analyst** - FTC, Raytheon – Harlow, UK
- **Information Security Engineer, Cisco** – Raleigh, NC,
- **Information Security Technical Consultant**, Dell – Reston, VA

of the current security posture of those workloads. According to the Palo Alto Networks report, the "top two security control challenges SecOps are struggling with are visibility into infrastructure security (forty-three percent) and compliance (thirty-eight percent)."

To obtain the proper level of visibility across your cloud workloads, you can't rely only on a well-documented set of processes; you must have the right set of tools. According to Palo Alto Networks, eighty-four percent of the respondents said that "traditional security solutions either don't work at all or have limited functionality." This leads to a conclusion that ideally you should evaluate your cloud provider's native cloud security tools before even starting to move to the cloud. But many current scenarios are far from the ideal, which means you need to evaluate the cloud provider's security tools while the workloads are already on it. This brings us to the discussion of two major categories of cloud security tools that are imperative these days:

- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)

Cloud security posture management

When talking about cloud security posture management, we are basically referring to three major pillars: visibility, monitoring, and compliance assurance. A CSPM tool should be able to look across all these pillars and provide capabilities to discover new and existing workloads (ideally across different cloud providers), identify misconfigurations, provide recommendations to enhance the security posture of cloud workloads, and assess cloud workloads to compare against regulatory standards and benchmarks. According to Gartner, a typical deployment pattern for CSPM has the layers shown in figure 2.[3]

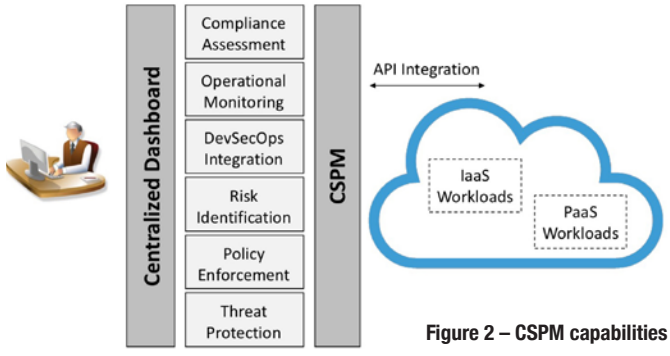

Figure 2 – CSPM capabilities

Each layer is responsible for retrieving the relevant data across the different workloads, rationalize it, and providing the output via a dashboard. Some layers may also have the capability to integrate with external work flows, for example, to send emails or to trigger remediation tasks in case a pre-determined threshold is reached. Table 1 has general consider-

3 Richard Bartley, "Comparing the Use of CASB, CSPM, and CWPP Solutions to Protect Public Cloud Services," Gartner (August 2018) – https://www.gartner.com/doc/3886773/comparing-use-casb-cspm-cwpp.

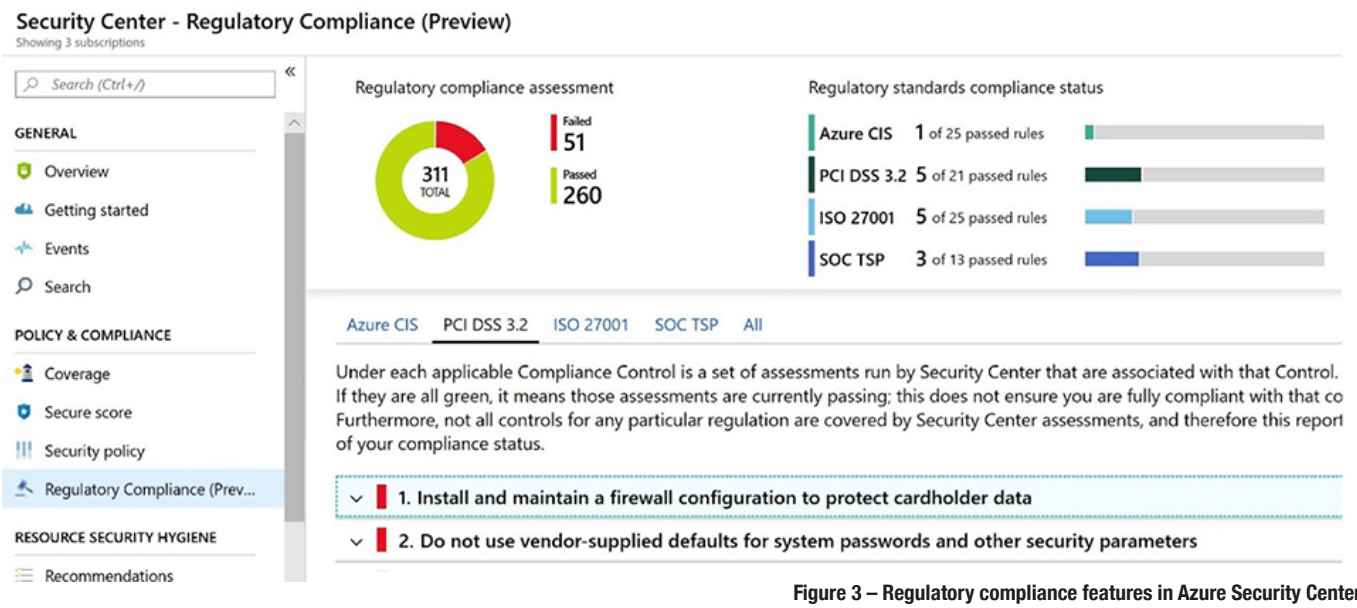

Figure 3 – Regulatory compliance features in Azure Security Center

CAPABILITY	CONSIDERATIONS
Compliance Assessment	Make sure the CSPM is covering the regulatory standards used by your company.
Operational Monitoring	Ensure that you have visibility throughout the workloads, and that best practices recommendations are provided.
DevSecOps Integration	Make sure it is possible to integrate this tool to existing work flows and orchestration. If it is not, evaluate the available options to automate and orchestrate the tasks that are critical for DevSecOps.
Risk Identification	How the CSPM tool is identifying risks and driving your workloads to be more secure? This is an important question to answer when evaluating this capability.
Policy Enforcement	Ensure that it is possible to establish central policy management for your cloud workloads and that you can customize and enforce it.
Threat Protection	How do you know if there are active threats in your cloud workloads? When evaluating the threat protection capability for CSPM, it is imperative that you can not only protect (proactive work) but also detect (reactive work) threats.

Table 1 – CSPM general considerations

ations for each one of those capabilities of the layered model descried in figure 2.

Some cloud platforms will offer native CSPM solutions that are capable of mapping different regulatory compliance models to your workloads and provide recommendations for security controls. The example shown in figure 3 is from the Azure Security Center regulatory and compliance feature, with the compliance control mapping for the monitored workloads located in Azure.

Cloud workload protection platform

By now you can already conclude that having a CSPM is an important step towards securing your cloud deployment. But there are other aspects of cloud security that need to be addressed including hardening, configuration, network security (firewall, segmentation), protection against exploits, application whitelisting, and other in-depth security capabilities. To address those needs, you will need to use a cloud workload protection platform (CWPP) tool. Gartner also exemplified a typical deployment pattern for CWPP, as shown in figure 4.[4]

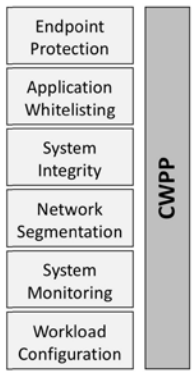

Figure 4 – CWPP deployment patterns

Cloud workload protection platforms that offer these deployment patterns en-

4 Ibid.

CAPABILITY	CONSIDERATIONS
Endpoint Protection	Make sure the CWPP can integrate with the current endpoint protection solution that is running on your IaaS workloads.
Application Whitelisting	Ensure that you can whitelist applications that are running in your IaaS deployments.
System Integrity	Make sure it is possible to monitor file integrity in Windows and Linux systems.
Network Segmentation	Ensure you can harden virtual network traffic used by your IaaS workloads.
System Monitoring	How do you monitor active events in Windows and Linux platforms? This is an important question that needs to be addressed by the CWPP. Ideally this should be seamless for IaaS workloads in the cloud, as well as on-premises resources in a hybrid cloud scenario.
Workload Configuration	How to deploy workload configuration in scale by leveraging security best practices, another important consideration that should be covered by the CWPP.

Table 2 – CWPP considerations

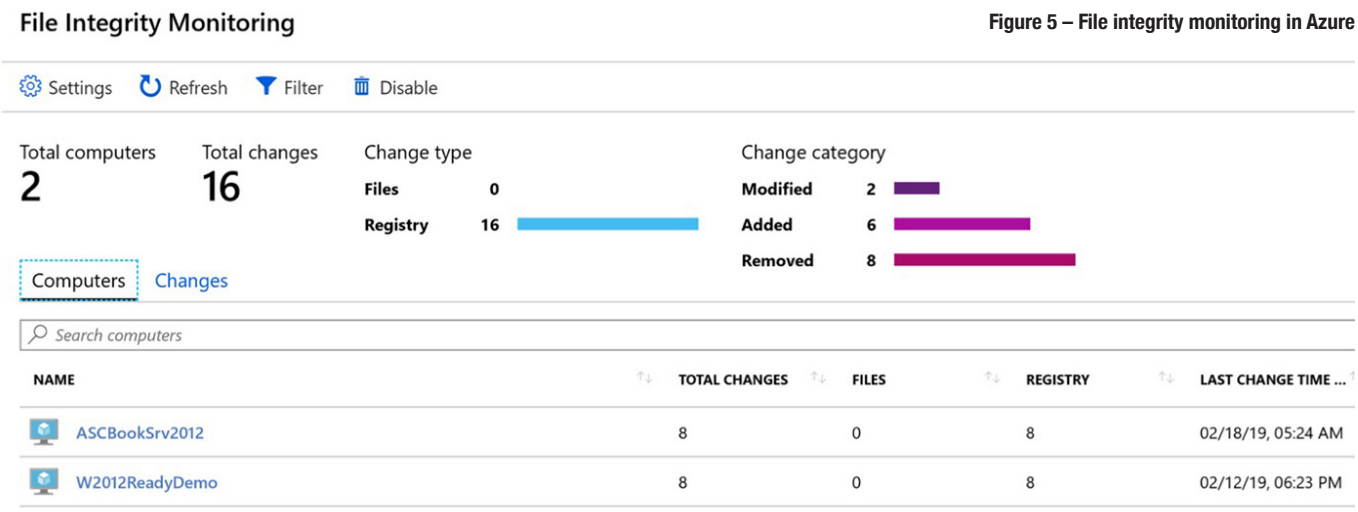

Figure 5 – File integrity monitoring in Azure

able customers to have more control and security over their enterprise workloads, containers, and storage across multiple IaaS public cloud deployments and also traditional on-premises data center environments (hybrid cloud scenario). Since CWPP is a more in-depth security protection, it can also have threat detections as part of the system monitoring capabilities. Let's review some important considerations for each one of those capabilities of the layered model descried in figure 4 (table 2).

Some cloud platforms will offer native CWPP solutions that are capable of mapping all suggested patterns described in table 2. Make sure to evaluate the options, as native cloud tools are usually able to offer some unique capabilities since the cloud provider owns the underlying infrastructure. The example shown in figure 5 is from the Azure Security Center file integrity monitoring capability that can monitor Windows and Linux platforms.

In order to provide in-depth security for your workloads, it is common that CWPP implementations are agent-based solutions. In a recent blog post published by Palo Alto Networks,[5] they reported that analysis done in cryptominer code used by Rocke group[6] identified that the malicious code was able to evade detection by uninstalling the cloud security protection and monitoring products from compromised Linux servers. Since this has the potential to become be a new attack vector against CWPP, it is imperative to verify with your CWPP vendor if they have the capability to detect this attempt to evade detection.

Conclusion

Cloud security should be tackled from different angles, and as demonstrated in this article, a single approach may not cover all aspects that will enhance the security posture while keeping in-depth monitoring of the different cloud workloads. For this reason, CSPM and CWPP are solutions that should be prioritized during the planning phase of your cloud migration. For existing cloud deployments, it is important to review the design patterns of existing workloads, and ensure that the CSPM and CWPP solutions are capable of addressing current and future needs.

About the Author

Yuri Diogenes, CISSP, MS in Cybersecurity Intelligence & Forensics Investigation, currently works for Microsoft as Senior Program Manager for Azure Security Center. Yuri is also a Professor for the Master of Science in Cybersecurity course from EC-Council University. You can follow Yuri on Twitter @yuridiogenes or his website yuridiogenes.us, yurid@microsoft.com.

5 Xingyu Jin and Claud Xiao, "Malware Used by 'Rocke' Group Evolves to Evade Detection by Cloud Security Products," Unit 42, PaloAlto Networks (Jan. 17, 2019) – https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evolves-to-evade-detection-by-cloud-security-products/.

6 Ed Targett, "This Malware Turns Off Your Cloud Security Tools," Computer Business Review (Jan. 1, 2019) – https://www.cbronline.com/news/rocke-group-malware.